Random number generation using environmental background electric noise · producing bit sequence from non-periodic amplitudes of detected 3 K black-body radiation in excess of threshold level

Publication number: DE4213988
Publication date: 1993-11-04

Inventor: HECHTENBERG ROLF-RENE (DE)
Applicant: HECHTENBERG ROLF RENE (DE)

Classification:
- international: ***G06F7/58; H03K3/84;*** **G06F7/58; H03K3/00;** (IPC1-7): G07C15/00; G06F7/58; H03K3/84
- european: G06F7/58R; H03K3/84
Application number: DE19924213988 19920429
Priority number(s): DE19924213988 19920429

Abstract of **DE4213988**

The number generating method involves picking-up cosmic radio noise picked by an antenna (2) for forwarding to a tuned receiver (1) whose output is digitised (3) in a processor (4) contg. a threshold-level circuit (5) and a bit serialiser (6). The bit sequence is transmitted to a computer (7). To forestall any attempt to manipulate the selection of random numbers the tuning of the receiver is varied at irregular intervals within the range of wavelengths from about 0.26 to 50 cm, within the spectrum of the background noise. USE/ADVANTAGE - Any number of successive random numbers can be generated with complete independence of any pattern.

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 42 13 988 A 1**

(51) Int. Cl.[5]:
G 07 C 15/00
G 06 F 7/58
H 03 K 3/84

(21) Aktenzeichen: P 42 13 988.0
(22) Anmeldetag: 29. 4. 92
(43) Offenlegungstag: 4. 11. 93

DE 42 13 988 A 1

(71) Anmelder:
Hechtenberg, Rolf-René, 2900 Oldenburg, DE

(74) Vertreter:
Schlagwein, U., Dipl.-Ing., Pat.-Anw., 61231 Bad Nauheim

(72) Erfinder:
gleich Anmelder

(56) Für die Beurteilung der Patentfähigkeit in Betracht zu ziehende Druckschriften:

DE	40 24 323 A1
DE	38 02 197 A1
DE	35 16 615 A1
DE	31 29 550 A1
SU	13 59 891 A1
SU	12 26 451 A

(54) Verfahren und Vorrichtung zur Gewinnung von Zufallszahlen

(57) Zur Gewinnung von Zufallszahlen wird das Hintergrundrauschen des Weltraumes aufgenommen. Anhand der wechselnden Amplituden dieses Rauschens werden mittels zumindest eines Schwellenwertes Bit-Folgen gewonnen, aus denen ein Prozessor zufällige Zahlen gewinnt.

DE 42 13 988 A 1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

BUNDESDRUCKEREI 09. 93 308 044/100

BNSDOCID: <DE_____4213988A1_I_>

Beschreibung

Die Erfindung betrifft ein Verfahren und eine Vorrichtung zur Gewinnung einer beliebigen Anzahl von Zufallszahlen.

Die Gewinnung von Zufallszahlen hat große praktische Bedeutung. Beispielsweise müssen bei Meinungsforschungen die Befragten nach Zufallskriterien ausgewählt werden. Auch bei der Wettersimulation oder anderen Simulationsvorgängen und bei der Verschlüsselung von Daten ist man auf Zufallszahlen angewiesen.

Bisher hat man Zufallszahlen mittels eines Computers nach bestimmten mathematischen Prinzipien ermittelt. Gemeinsam ist jedoch allen Systemen zur Ermittlung von Zufallszahlen, daß nach einer sehr großen Anzahl von aufeinanderfolgenden Zahlen die ihrer Gewinnung zugrundeliegende mathematische Gesetzmäßigkeit erkennbar wird. Man spricht deshalb von Pseudozufallszahlen.

Der Erfindung liegt das Problem zugrunde, ein Verfahren zur Ermittlung von Zufallszahlen zu entwickeln, bei denen auch bei einer beliebig großen Anzahl von aufeinanderfolgenden Zahlen keine Gesetzmäßigkeit eintritt. Weiterhin soll eine Vorrichtung zur Durchführung dieses Verfahrens geschaffen werden.

Das erstgenannte Problem wird erfindungsgemäß dadurch gelöst, daß die elektromagnetische Hintergrundstrahlung des Weltraumes empfangen und aus den zumindest einen Schwellenwert übersteigenden Amplituden dieser Hintergrundstrahlung eine Bit-Folge erzeugt wird.

Durch Heranziehung dieser Hintergrundstrahlung, welche auch 3°-Kelvin-Strahlung genannt wird, kann man aus Signalen, welche von einer unendlich großen Anzahl von Körpern ausgehen, echte Zufallszahlen mit geringem Aufwand und in beliebig großer Anzahl gewinnen.

Besonders vorteilhaft ist es, wenn zur Gewinnung aufeinanderfolgender Bit-Folgen mehrere Schwellenwerte vorgesehen werden.

Wenn das erfindungsgemäße Verfahren bekannt geworden ist und Verbreitung gefunden hat, dann wäre es denkbar, daß zur bewußten Verfälschung der gewonnenen Zufallszahlen ein anderer im Frequenzbereich des Hintergrundrauschens Störsignale sendet. Eine solche Manipulation kann auf einfache Weise verhindert werden, wenn zur Gewinnung der Zufallszahlen in unregelmäßiger Reihenfolge unterschiedliche Frequenzen der Hintergrundstrahlung berücksichtigt werden.

Das zweitgenannte Problem, nämlich die Schaffung einer Vorrichtung zur Durchführung des Verfahrens zur Gewinnung einer großen Anzahl von Zufallszahlen, wird erfindungsgemäß dadurch gelöst, daß die Vorrichtung einen Empfänger für eine Hintergrundstrahlung im Bereich von etwa 3° Kelvin, einen nachgeschalteten Prozessor mit einem Analog/Digital-Wandler, einer Schwellenwertschaltung und einer Bit-Anreihung zur Umwandlung der Digitalsignale in eine Bit-Folge aufweist.

Die Erfindung ist für den Elektroniker sehr einfach ausführbar. Zu ihrer weiteren Verdeutlichung wird nachfolgend auf die Zeichnung Bezug genommen. Diese zeigt in

Fig. 1 ein Diagramm, welches die Amplitude des Hintergrundrauschens über die Zeit zeigt,

Fig. 2 ein Blockdiagramm der erfindungsgemäßen Vorrichtung.

In **Fig.** 1 ist die y-Achse übereinander in achtzehn

Bereiche abwechselnd mit 0 und 1 eingeteilt. Die eingetragene Linie zeigt die Amplitude einer ausgewählten Frequenz des Hintergrundrauschens. Die x-Achse ist in 37 Meßbereiche eingeteilt. Man erkennt, wie aufgrund der zufällig wechselnden Amplitude duale Zahlen für die Bit-Folge gewonnen werden können.

Das Blockschaltbild gemäß **Fig.** 2 zeigt einen als Radiowellenempfänger ausgebildeten Empfänger 1 mit einer Antenne 2. Dieser Empfänger 1, der auf die Frequenz der Hintergrundstrahlung des Weltalls eingestellt ist, gibt die empfangenen Amplituden an einen Analog/Digital-Wandler 3 eines Prozessors 4 weiter. Eine Schwellenwertschaltung 5 ermittelt daraus binäre Zahlen, welche in einer Bit-Anreihung 6 zu Bit-Folgen aneinandergereiht werden. Diese Bit-Folgen werden an einen Computer 7 übertragen.

Um eventuellen Manipulationen der Auswahl der Zufallszahlen vorzubeugen, ändert der Prozessor 4 in unregelmäßigen Abständen die Empfangsfrequenz. Da die Hintergrundstrahlung nicht auf einen engen Bereich begrenzt ist, können sich die Empfangsfrequenzen etwa zwischen 50 cm und 0,26 cm Wellenlänge bewegen.

Patentansprüche

1. Verfahren zur Gewinnung einer beliebigen Anzahl von Zufallszahlen, **dadurch gekennzeichnet,** daß die elektromagnetische Hintergrundstrahlung des Weltraumes empfangen und aus den zumindest einen Schwellenwert übersteigenden Amplituden dieser Hintergrundstrahlung eine Bit-Folge erzeugt wird.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß zur Gewinnung aufeinanderfolgender Bit-Folgen mehrere Schwellenwerte vorgesehen werden.
3. Verfahren nach den Ansprüchen 1 oder 2, dadurch gekennzeichnet, daß zur Gewinnung der Zufallszahlen in unregelmäßiger Reihenfolge unterschiedliche Frequenzen der Hintergrundstrahlung berücksichtigt werden.
4. Vorrichtung zur Durchführung des Verfahrens nach einem oder mehreren der vorangehenden Ansprüche, dadurch gekennzeichnet, daß sie einen Empfänger (1) für eine Hintergrundstrahlung im Bereich von etwa 3° Kelvin, einen nachgeschalteten Prozessor (4) mit einem Analog/Digital-Wandler (3), einen Schwellenwertschaltung (5) und einer Bit-Anreihung (6) zur Umwandlung der Digitalsignale in eine Bit-Folge aufweist.

Hierzu 1 Seite(n) Zeichnungen

– Leerseite –

Nummer: DE 42 13 988 A1
Int. Cl.[5]: G 07 C 15/00
Offenlegungstag: 4. November 1993

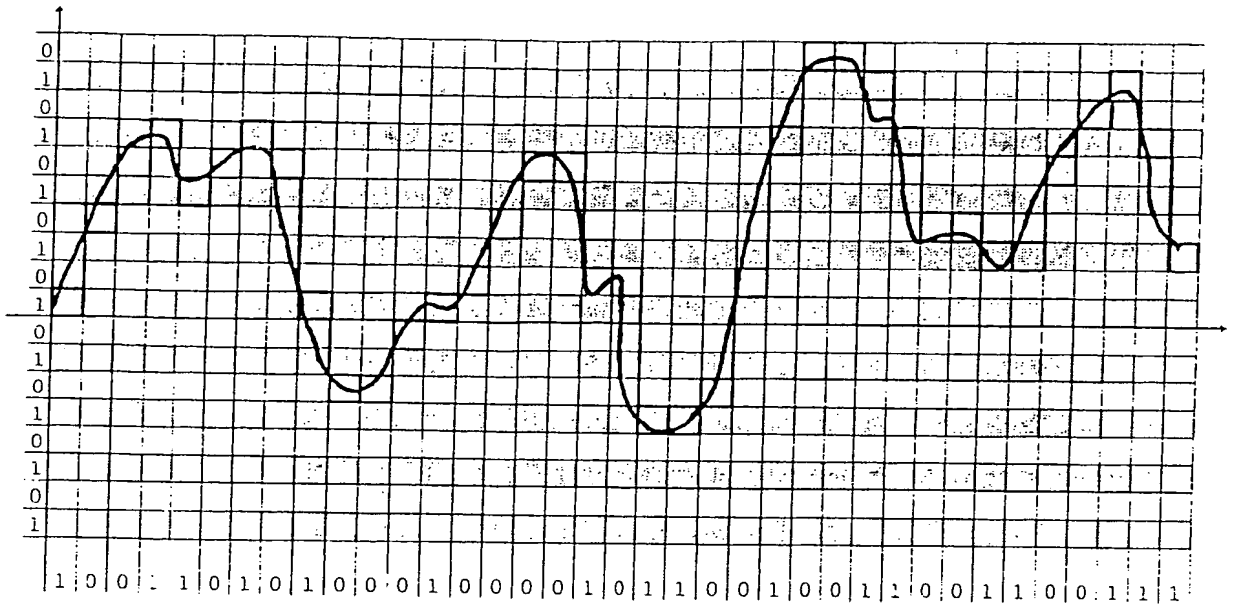

Fig. 1

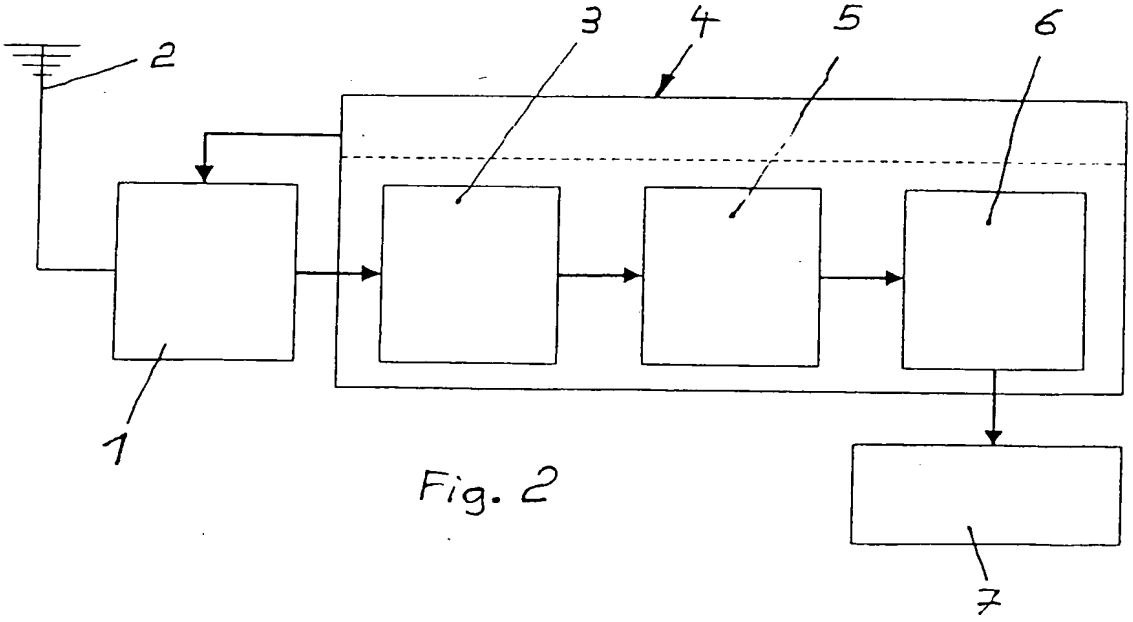

Fig. 2